(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

Offenlegungsschrift

(10) DE 100 09 209 A 1

(51) Int. Cl.[7]:
G 02 F 3/00
H 04 L 9/08
H 04 B 10/12
G 02 F 1/21

(21) Aktenzeichen: 100 09 209.8
(22) Anmeldetag: 26. 2. 2000
(43) Offenlegungstag: 6. 9. 2001

DE 100 09 209 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Dultz, Wolfgang, Prof, Dr., 65936 Frankfurt, DE; Schmitzer, Heidrun, Dr., 93051 Regensburg, DE; Beresnev, Leonid, Dr., Columbia, US; Dultz, Gisela, 65936 Frankfurt, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	198 33 330 A1
US	53 15 422
US	52 43 649
EP	07 22 640 B1
EP	06 76 110 B1
WO	95 07 584 A1

TOWNSEND,Paul D.: A quantum key distribution channel based on optical fibre. In: Journal Of Modern Optics, 1994, Vol.41, No.12, S.2425-2433;
RARITY,J.G., et.al.: Quantum random-number generation and key sharing. In: Journal Of Modern Optics, 1994, Vol.41, No.12, S.2435-2444;
BENNETT,Charles H.: Quantum Cryptography Using
Any Two Nonorthogonal States. In: Physical Review Letters, Vol.68, No.21, May 1992, S.3121-S.3124;
TOWNSEND,P.D., et.al.: Single Photon Interference In 10km Long Optical Fibre Interferometer. In: Electronics Letters, 1st April 1993, Vol.29, No.7, S.634,635;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Vorrichtung zur Erzeugung, Addition und Subtraktion digitaler Folgen optischer Pulse und Verfahren zur sicheren Übertragung von Nachrichten

(57) Damit bei einer elektrooptischen Vorrichtung und einem Verfahren zur sicheren Übertragung von Nachrichten mit optischen Signalen, die Addition und/oder Subtraktion von binären optischen Pulsfolgen durchgeführt werden kann, wird ein Interferometer eingesetzt, bei welchem zumindest ein elektrooptischer Schalter oder Modulator in einem der Teilzweige des Interferometers angeordnet ist.

DE 100 09 209 A 1

Beschreibung

Die Erfindung betrifft eine Vorrichtung zur Erzeugung, Addition und Subtraktion digitaler, vorzugsweise binärer Folgen optischer Pulse und ein Verfahren zur sicheren Übertragung von Nachrichten.

Eines der großen Probleme in der Zukunft der Telekommunikation wird darin bestehen, die Sicherheit der Nachrichtenübertragung zu erhöhen und insbesondere die zu übertragenden Nachrichten vor unbefugtem Abhören oder ungewollten Verfälschungen zu bewahren. Eine sicheres Verfahren umfasst die Verschlüsselung der binär kodierten Nachricht durch Addition zu einem stochastischen binären Schlüssel, der so lang ist wie die Nachricht selbst. Es entsteht hierbei eine stochastische binäre Folge, die nur durch Subtraktion des Schlüssels entziffert werden kann. Dieses Verfahren, welches im Englischen "one time pad" heißt, ist absolut sicher, wenn der Schlüssel, der so lange wie die Nachricht selbst ist, nur einmal verwendet wird.

Der Erfindung liegt die Aufgabe zu Grunde, das vorstehend beschriebene Verfahren auf zuverlässige Weise auch mit optischen Signalen zu ermöglichen.

Diese Aufgabe wird durch eine Vorrichtung nach Anspruch 1 und ein Verfahren gemäß Anspruch 12 gelöst.

Ein erfindungsgemäß bevorzugtes Kommunikationssystem ist in Anspruch 13 definiert.

Optische Signale sind aufgrund ihrer prinzipiell extrem hohen Ausbreitungsgeschwindigkeit, zusammen mit deren parallelen Verarbeitungsmöglichkeiten und der Kombinierbarkeit mit vorhandenen elektronischen nachrichtentechnischen Geräten von stark zunehmendem Interesse.

Die stochastische Binärfolge, die als Schlüssel dient, kann zum Beispiel mit Hilfe eines optischen Zufallsgenerators generiert werden oder kann elektronisch gewonnen und in ein optisches Signal gewandelt werden.

Die Erfindung wird nachfolgend anhand bevorzugter Ausführungsformen und unter Bezugnahme auf die beigefügten Zeichnungen detaillierter beschrieben.

Es zeigen:

Fig. 1: ein Schema des Additions- bzw. Subtraktionselements auf der Grundlage eines Mach-Zehnder Interferometers zur genauen Abstimmung kann der Spiegel S3 z. B. durch ein Piezoelement hin und her gefahren werden,

Fig. 2: eine Qualitative Darstellung der Addition der Pulsfolge A1 zur Pulsfolge B1. 01 stellt die addierte Folge im Ausgang 01 des Interferometers aus Fig. 1 dar, wobei 02 ist die Pulsfolge im anderen Ausgang 02 darstellt.

Detaillierte Beschreibung der Erfindung

Die Erfindung umfaßt optische Anordnungen, die es erlauben, zwei Lichtpulsfolgen zu generieren und dann optisch zu addieren oder zu subtrahieren.

Bei einer Ausführungsform der hier beschriebenen Erfindung werden, vorab in Kürze zusammengefasst, zwei optische Pulsfolgen A und B aus vorliegenden elektronischen Pulsfolgen generiert. Eine davon trägt z. B. die Information, die andere den stochastischen Schlüssel. Zur optischen Addition der Zufallsfolge zu der optischen Pulsfolge, die die Information enthält, dient die Interferenz zwischen den beiden synchronen Pulsfolgen. Das hierzu benötigte Element wird im folgenden eingehender beschrieben.

Das binäre Additionselement soll die direkte Addition optischer Binärinformationen ermöglichen, also: $0 + 0 = 0$, $1 + 0 = 0 + 1 = 1$, $1 + 1 = 0$. Da die Subtraktion im binären, einziffrigen Zahlenraum der Addition entspricht, kann das Element damit auch subtrahieren: $0 - 0 = 0$, $1 - 0 = 0 - 1 = 1$, $1 - 1 = 0$.

Das hier beschriebene optische Element erzeugt aus einem kontinuierlichen, ungepulsten, kohärenten Lichtstrahl oder einer monotonen Folge kohärenter optischer Pulse zwei unterschiedlich kodierte binäre Pulsfolgen, wobei die Kodierung extern beliebig vorgegeben werden kann. Die beiden Pulsfolgen A, B werden anschließend interferometrisch addiert bzw. subtrahiert und als Ausgangssignale 01 und 02 in dem Ausgang 01 bzw. 02 erhalten.

Fig. 1 zeigt als erste bevorzugte Ausführungsform eine Mach-Zehnder Interferometeranordnung, die es erlaubt mit Hilfe von zwei elektrooptischen Schaltern A1, B1, die elektronisch vorliegenden Pulsfolgen einer monotonen, kohärenten, optischen Pulsfolge oder einem kontinuierlichen, kohärenten Lichtstrahl im Eingang E des Interferometers aufzuprägen.

Es sind erfindungsgemäß ferner zweidimensionale Signale, verarbeitbar, wenn die elektrooptischen Schalter und Modulatoren mit einem abbildendem System eingesetzt werden. Derartige Systeme können beispielsweise mit einer Sammellinse aufgebaut werden, die außerhalb des Interferometers angeordnet ist und in deren Objektebene die zweidimensionaler elektrooptischen Modulatoren oder Schalter stehen. Ferner können zwei sehr ähnliche Sammellinsen innerhalb des jeweiligen Teilzweigs des Interferometers angeordnet sein, in jedem Falle werden dann die Nutzsignale in der Bildebene des optischen Systems erhalten.

Bei hoher örtlicher Kohärenz, dies bedeutet bei einer kleinen, bzw. punktförmigen Lichtquelle oder sehr paralleler optischer Strahlung sind auch zeitlich stark inkohärente Signale, dies bedeutet breitbandige Signale möglich, da das Mach-Zehnder-Interferometer und die nachfolgend namentlich benannten Interferometer sogenannte Weißlicht-Interferomenter sind, welche bei einer optischen Wegdifferenz der beiden Interferometerarme von weniger als etwa 3 µm hervorragend für die Erzeugung von Weißlicht-Interferenzmustern geeignet sind. Dadurch kann beispielsweise ein einziges stochastisches Signal, das in einem der Teilzweige eingespeist wird für eine Vielzahl spektral getrennter optischer Frequenzen verwendet werden. Bei einem Abgleich der optischen Weglänge um den Differenzbetrag etwa gleich Null oder kleiner als 0,5 µm herum, kann im wesentlichen fast das gesamte optische Spektrum gleichzeitig ausgenutzt werden, da diese Bedingung dann etwa der optischen destruktiven Weißlichtinterferenz entspricht.

Gemäß Fig. 1 spaltet der Spiegel S1 die monotone Pulsfolge in zwei monotone Pulsfolgen von halber Intensität auf. Die Modulatoren A1, B1 prägen den beiden monotonen Pulsfolgen den, die jeweilige Information enthaltenden Kode auf.

Der eine Kode ist z. B. ein stochastischer binärer Schlüssel, der andere enthält die binär verschlüsselte Nachricht. Eine der beiden Pulsfolgen erhält eine Phasenverschiebung von einer halben Wellenlänge z. B. durch eine $\lambda/2$ Verzögerung.

Die beiden Pulsfolgen werden dann am Spiegel S2 zur Interferenz gebracht. Ist das Interferometer richtig abgestimmt, so verläßt am Ausgang 01 eine Pulsfolge das Interferometer, die einer Summe oder Differenz der binäre Pulsfolgen A, B in den beiden Armen des Interferometers entspricht. Das Interferometer ist dabei so abgestimmt, daß die optischen Wege in den beiden Armen gleich sind.

Die zusätzliche $\lambda/2$ Verzögerung bewirkt, daß Pulse, die in beiden Armen auftreten, so interferieren, daß diese das Interferometer am Ausgang 02 verlassen.

Pulse, die nur in einem Arm auftreten, verlassen das Interferometer in beiden Ausgängen 01 und 02.

Pulse, die in keinem der Arme auftreten, treten in keinem der Ausgänge auf. Daher findet man nur im Ausgang 01 eine

binäre Summe bzw. Differenz der beiden Pulsfolgen.

Läßt man die λ/2 Verzögerungsplatte weg, so tritt die Summe bzw. Differenz im Ausgang 02, nicht aber im Ausgang 01 auf.

Wichtig ist es, daß die elektrooptischen Schalter in beiden Armen die gleichen zusätzlichen optischen Wege einführen. Ist dies nicht der Fall, so kann man den optischen Weg in einem der Arme, z. B. durch Verschieben des Spiegels S3 verlängern oder verkürzen, so daß die optischen Wege in den Armen wieder gleich werden.

In **Fig.** 2 ist eine Addition zweier Pulsfolgen A, B mit Hilfe dieses Verfahrens als Beispiel aufgezeichnet. Die Pulsfolge A wird zur Pulsfolge B addiert, synchrone Pulse in beiden Folgen werden im Ausgang 02 beobachtet. Die Anordnung **Fig.** 1 mit λ/2 Verzögerung wurde dabei benutzt.

Die Pulshöhen in **Fig.** 2 stellen die Verhältnisse nur qualitativ dar und sind nicht maßstabsgetreu.

Das Prinzip des hier beschriebenen Additions- bzw. Subtraktionselementes besteht also darin, daß zwei kohärente optische Pulse durch eine Phasenverschiebung von λ/2 interferometrisch in einem Ausgang zu Null gemacht werden und das Interferometer in einem anderen Ausgang verlassen. Dabei kommt es im wesentlichen nicht auf die Art des Interferometers an.

Alle Zweistrahlinterferometer können als Grundlage für das Additions- bzw. Subtraktionselement dienen. Mögliche weiteren Anordnungen neben dem Mach-Zehnder-Interferometer sind z. B. das Michelson-Interferometer oder das Jamin-Interferometer.

Notwendig ist nur die räumliche Aufteilung eines kohärenten Lichtstrahls in zwei Teile, das Aufprägen der beiden Pulskodierungen auf die beiden Teilstrahlen und das anschließende interferometrische Überlagern entweder ohne Phasenverschiebung oder mit einer Phasenverschiebung von λ/2 je nachdem, welchen Ausgang des Interferometers man benutzen will.

Es können bei monochromatischem Licht auch ganze Vielfache der Wellenlängen zu diesen Phasenverschiebungen addiert werden. Solange die gesamte optische Wegdifferenz innerhalb der Kohärenzlänge bleibt, gilt diese Aussage auch für polychromatisches Licht. Die Technik dafür ist vorhanden und umfasst beispielsweise Verzögerungsplatten oder bewegliche Elemente (z. B. Spiegel) des Interferometers.

Ferner ist es im Sinne der Erfindung nicht nötig, daß am Eingang des Interferometers bereits ein monotoner Pulszug eingespeist wird. Die Pulserzeugung kann beispielsweise auch durch die elektrooptischen Modulatoren oder Schalter in den Armen des Interferometers zusammen mit der Kodierung erfolgen.

Der Einsatz des Additionselementes in der Telekommunikation macht es sinnvoll, alle optischen Elemente durch entsprechende Elemente aus optischen Glasfasern zu ersetzen, z. B. die halbdurchlässigen Spiegel durch Faserkoppler usw.

Auch eine Realisierung der Erfingung in integrierter Optik ist auf vorteilhafte Weise möglich.

Patentansprüche

1. Elektrooptische Vorrichtung zur Erzeugung, Addition und/oder Subtraktion von binären optischen Pulsfolgen, **gekennzeichnet durch** ein Interferometer, bei welchem zumindest ein elektrooptischer Schalter oder Modulator in einem der Teilzweige des Interferometers angeordnet ist.

2. Elektrooptische Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß das Interferenzmuster durch eine Phasenverschiebung in dem elektrooptischen Schalter oder Modulator entsprechend einem digitalen optischen Signal erzeugt ist.

Schalter oder Modulator erzeugt ist.

3. Elektrooptische Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß das Interferenzmuster durch eine Phasenverschiebung in dem elektrooptischen Schalter oder Modulator entsprechend einem stochastischen digitalen optischen Signal erzeugt ist.

4. Elektrooptische Vorrichtung nach Anspruch 3, dadurch gekennzeichnet, daß die Interferenz zwischen dem optischen Signal in dem einen Teilzweig mit dem elektrooptischen Schalter oder Modulator und einem eingespeisten binären optischen Signal erzeugt ist.

5. Elektrooptische Vorrichtung nach Anspruch 3, dadurch gekennzeichnet, daß ein weiterer elektrooptischer Modulator oder Schalter in dem weiteren Zweig des Interferometers angeordnet ist.

6. Elektrooptische Vorrichtung nach Anspruch 4, dadurch gekennzeichnet, daß das binäre optische Signal durch den weiteren elektrooptischen Schalter oder Modulator erzeugt ist.

7. Elektrooptische Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß das Interferometer ein Mehrstrahlinterferometer und insbesondere ein Zweistrahlinterferometer ist.

8. Elektrooptische Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, daß das Interferometer ein Mach-Zehnder-, ein Michelson- oder ein Jamin-Interferometer ist.

9. Elektrooptische Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die Modulatoren oder Schalter zweidimensionale ortsaufgelöste Modulatoren oder Schalter sind.

10. Elektrooptisches Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die einzelnen optischen Elemente faseroptische Elemente sind.

11. Elektrooptische Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die optischen Elemente integriert-optische Elemente sind.

12. Verfahren zur sicheren Übertragung von Nachrichten mittels optischer Signale, bei welchem die Erzeugung von optischen Pulsfolgen in einer Vorrichtung gemäß einem der Ansprüche von 1 bis 10 erfolgt.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß in einem Zweistrahlinterferometer mit elektrooptischen Schaltern oder Modulatoren, in den beiden Armen Phasenverschiebungen erzeugt werden und immer wenn eine Überlagerung von zwei Lichtpulsen am Ausgang des Interferometers vorliegt, der genutzte Ausgang die destruktive Interferenz der beiden Pulse enthält.

14. Kommunikationssystem umfassend eine Vorrichtung und ein Verfahren nach einem der vorstehenden Ansprüche.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 09 209 A1
Int. Cl.[7]: G 02 F 3/00
Offenlegungstag: 6. September 2001

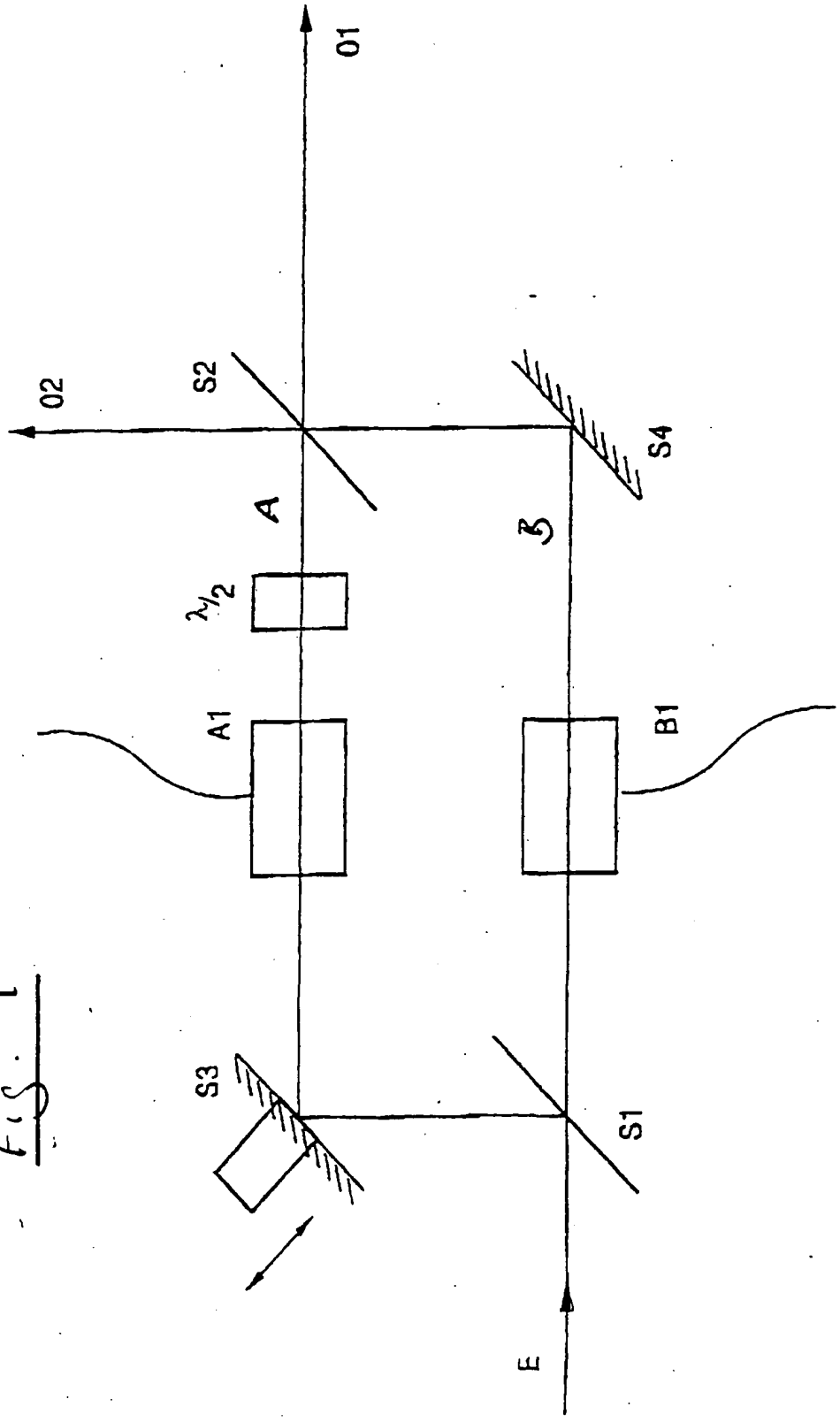

Fig. 1

Nummer: DE 100 09 209 A1
Int. Cl.[7]: G 02 F 3/00
Offenlegungst 6. September 2001

Fig. 2